

AFFIDAVIT

I, Than Trung Nguyen, having been first duly sworn, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with Internal Revenue Service – Criminal Investigation (“IRS-CI”) since October 2018. My responsibilities include the investigation of tax fraud, money laundering, and the illegal structuring of financial transactions, among other federal criminal violations. I hold a bachelor’s degree in economics from Boston College and masters degrees in accounting and business administration from the University of Massachusetts, Boston. I have received extensive training in financial investigative techniques, money laundering, Bank Secrecy Act violations and in the law of search and seizure under the Fourth Amendment.

2. I am investigating Bill Dessaps (“Dessaps”) for his involvement in wire fraud, bank fraud, bank and wire fraud conspiracy, false statements to a financial institution, theft of government funds, concealment money laundering, unlawful financial transactions, and money laundering conspiracy in violation of 18 U.S.C. §§ 1343, 1344, 1349, 1014, 641, 1956(a)(1)(B)(i), 1956(h), and 1957 (“the Target Offenses”).

3. I submit this affidavit in support of applications for:

a. a criminal complaint charging Dessaps with wire fraud conspiracy and money laundering conspiracy, in violation of 18 U.S.C. § 1349 and 1956(h), respectively, and a warrant to arrest Dessaps on these charges—because the investigation reveals that Dessaps’s submitted fraudulent loan applications and later engaged in financial transactions with the fraudulently obtained loan proceeds; and

b. a warrant to search 21 Justin Drive in South Easton, Massachusetts 02375 (the “Subject Premises”), including the attached three-car garage, for evidence, fruits, and

instrumentalities of the Target Offenses, including, among other evidence, Dessaps's mobile phone with the assigned number (781) 708-5011; and

c. a warrant to seize a black 2014 Rolls Royce Wraith bearing vehicle identification number ("VIN") SCA665C54EUX84378 (the "Rolls Royce"), pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 982(a)(1), and 28 U.S.C. § 2461(c).

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit does not set forth all facts developed during the course of this investigation and does not set forth all of my knowledge about this matter. It is intended to show that there is probable cause to believe that Dessaps has committed the Target Offenses and that there is probable cause for the requested warrants.

PROBABLE CAUSE

Relevant Individuals and Entities

At all times relevant to this affidavit:

5. Dessaps lived in Bridgewater, Massachusetts. Financial records and records maintained by the Massachusetts Secretary of the Commonwealth and the Internal Revenue Service ("IRS") list his residence as a home on Plymouth Street in Bridgewater (the "Bridgewater Address").

6. ABC Tech Squad Inc., formerly ABC Tech Squad LLC ("ABC Tech") was a used car dealership in Abington, Massachusetts. Dessaps registered ABC Tech with the Massachusetts Secretary of the Commonwealth on April 6, 2015. Dessaps listed himself and his brother as the business's managers on the initial registration, and he listed both his and his brother's address as the Bridgewater Address.

7. Recruiter 1, Recruiter 2, and Recruiter 3 were residents of Florida.

8. The U.S. Small Business Administration (“SBA”) was an agency of the United States government authorized to enable and provide for loans, guaranteed by the government, both directly and through banks, credit unions, and other lenders.

9. TD Bank was based in New Jersey and insured by the Federal Deposit Insurance Corporation (“FDIC”). It was an approved lender of Paycheck Protection Program (“PPP”) loans, which are described below.

10. Kabbage Inc. (“Kabbage”) was based in California. It was also an approved PPP lender.

11. Eastern Bank was based in Massachusetts. It was also an approved PPP lender.

Overview of Federal COVID-19 Relief Programs

12. The Coronavirus Aid, Relief, and Economic Security (“CARES”) Act was a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to Americans suffering the economic effects of the COVID-19 pandemic.

13. The CARES Act authorized forgivable loans to small businesses and non-profits for job retention and certain other expenses through the PPP.

14. In order to obtain a PPP loan, a qualifying business had to submit a PPP loan application signed by an authorized representative of the business. The PPP loan application required the business, through its authorized representative, to acknowledge the program rules and make certain affirmative certifications. In the PPP loan application, the small business, through its authorized representative, had to state, among other things, its (i) number of employees and (ii) average monthly payroll expenses. These figures were used to calculate the amount of a PPP loan the business was eligible to receive; typically, a business was eligible to receive two-and-a-half

times its average monthly payroll expenses. In addition, businesses applying for a PPP loan had to provide documentation of their payroll expenses.

15. A PPP loan application had to be processed by an authorized SBA lender. If a PPP loan application was approved, the participating lender funded the PPP loan using its own monies, which were 100 percent guaranteed by the SBA. Data from the application was regularly transmitted by the lender to the SBA in the course of processing the loan.

16. PPP loan proceeds had to be used by the business on certain permissible expenses, including payroll costs, interest on mortgages, rent, and utilities. The PPP allowed the interest and principal on the PPP loan to be entirely forgiven if the business spent the loan proceeds on these permissible expenses within a designated period of time and used a certain percentage of the PPP loan proceeds on payroll expenses.

Overview of the Scheme

17. Between May and June 2020, Dessaps submitted or caused to be submitted at least three PPP applications on behalf of ABC Tech. On the first two applications, Dessaps reported that ABC Tech had three or four employees and total monthly payroll expenses of, at most, \$15,000. As a result of the second of these applications, ABC Tech received a PPP loan of \$12,450 from Eastern Bank.

18. Less than a month later, however, Dessaps caused the submission of a third PPP application that falsely reported that ABC Tech had 40 employees and total monthly payroll expenses of \$334,720. As a result of this application, Kabbage disbursed \$836,800 to ABC Tech on June 5, 2020.

19. After receiving PPP funds, Dessaps issued checks to individuals to create the appearance of payroll expenses that would qualify for PPP loan forgiveness. Dessaps then used

most of the PPP funds to purchase the Subject Premises and the Rolls Royce, to pay \$32,000 to a breeder of French bulldogs, and to fund other personal expenses.

The TD Bank and Eastern Bank Applications

20. Bank records indicate that, on or about May 6, 2020, Dessaps signed and submitted a PPP application for ABC Tech to TD Bank. This application represented that ABC Tech had four employees and average monthly payroll expenses of \$15,000. Based on these payroll expenses, the application sought a PPP loan of \$37,500 (*i.e.*, two-and-a-half times the business's reported monthly payroll expenses). In support of this application, Dessaps provided TD Bank, with a copy of a 2018 Form 1040 (U.S. Individual Income Tax Return) Schedule 1 (Additional Income and Adjustments to Income), on which Dessaps reported to the IRS a net business income of \$18,600.

21. On at least three occasions between May 6 and May 20, 2020, TD Bank emailed Dessaps and requested that he provide additional documentation of ABC Tech's payroll, such as IRS Forms 940 (Employer's Annual Federal Unemployment Tax Return) or 941 (Employer's Quarterly Federal Tax Return). According to bank records, Dessaps never submitted additional documentation to TD Bank.

22. Bank records indicate that Dessaps submitted a second PPP application for ABC Tech, to Eastern Bank, on or about May 8, 2020. On this second application, Dessaps reported that ABC Tech had three employees and average monthly payroll expenses of just \$4,980. Based on this amount, the application sought a PPP loan of \$12,450. In support of this application, Dessaps provided Eastern Bank with a purported copy of a 2019 Form 1040 Schedule C (Profit or

Loss from Business). On the Schedule C, Dessaps reported gross income from ABC Tech of \$1,919,503 and a net profit of \$59,771. Dessaps left the Schedule C line for wages blank.¹

23. Bank records indicate that Eastern Bank approved Dessaps's second loan application and deposited \$12,450 into ABC Tech's bank account at Eastern Bank on or about May 18, 2020.

24. On or about May 26, 2020, Dessaps withdrew the TD Bank application and advised TD Bank that Eastern Bank had funded a PPP loan for ABC Tech.

The Fraudulent Kabbage Application

25. According to business records, Kabbage received a PPP application for ABC Tech only weeks later, on or about June 3, 2020. Like the applications submitted to TD Bank and Eastern Bank, this application identified Dessaps as the sole owner of ABC Tech, listed ABC Tech's address (the "Abington Address") as the business's address, and listed the Bridgewater Address as Dessaps's personal address.

26. The PPP application included a certification by the applicant confirming the applicant's understanding of the following statement, among others: "During the period beginning on February 15, 2020 and ending on December 31, 2020, the Applicant has not and will not receive another loan under the Paycheck Protection Program." At the time that the application was submitted to Kabbage, ABC Tech had already received PPP funds from Eastern Bank and withdrawn the PPP application pending with TD Bank.

27. In contrast to the applications that Dessaps submitted to TD Bank and Eastern Bank the month prior, the Kabbage application represented that ABC Tech had 40 employees and

¹ The purported Schedule C that Dessaps submitted to Eastern Bank was not the Schedule C that Dessaps later filed with the IRS, which investigators obtained and reviewed pursuant to an *ex parte* order.

average monthly payroll expenses of \$334,720. Based on these amounts, the application sought a PPP loan of \$836,800.

28. The supporting documentation for the application submitted to Kabbage included a photocopy of Dessaps's Massachusetts driver's license, showing the Bridgewater Address, and a License for Sale of Used Articles from the Town of Abington, Massachusetts for ABC Tech. The supporting documentation also included a purported copy of a 2019 Form W-3 (Transmittal of Wage and Tax Statements)² for ABC Tech. This form indicated that ABC Tech's gross payroll expenses in 2019 were \$3,840,000 and that the company withheld \$384,000 in federal income taxes. The Form W-3 also reported that ABC Tech paid \$238,080 in Social Security Wages and withheld that same amount in Social Security taxes, and that ABC Tech paid \$55,680 in Medicare wages and withheld that same amount in Medicare taxes.

29. According to business records, Kabbage approved the application and disbursed a PPP loan of \$836,800 to ABC Tech two days later, on or about June 5, 2020.

30. Based on my review of this loan application, business records related to other loan applications, and the investigation to date, I have determined that Dessaps caused the submission of this PPP application to Kabbage through others, including Recruiter 1 and Recruiter 2, in order to obtain an additional PPP loan to which ABC Tech was not entitled (and in amount for which ABC Tech was never eligible):

a. I have reviewed bank records, business records, internet service records, telephone records, and email communications. Based on my review of these records, I have concluded that Recruiter 2 submitted fraudulent PPP applications for Dessaps and other individuals; that Recruiter

² Form W-3 is used to summarize and transmit to the Social Security Administration all Form W-2s (Wage and Tax Statement) issued by a business for a calendar year. The amounts reported on a business's Form W-3 typically represent all wages the business paid during the year.

1 and Recruiter 3 identified potential borrowers, including Dessaps, to receive fraudulent PPP loans from applications submitted by Recruiter 2; and that Recruiter 1, Recruiter 2, and Recruiter 3 received kickback payments of “commissions” from the borrowers who received PPP funds as a result.

b. Bank records demonstrate that shortly after receiving PPP funds from Kabbage, Dessaps sent two checks totaling \$28,000 (\$14,000 each) from the TD Bank account that received the PPP funds to Recruiter 1’s purported not-for-profit organization in Florida. The memo line on the first check, dated June 9, 2020, stated “payroll check.” The memo line of the second check, dated June 12, 2020, read “services.” Shortly after receiving the first check, on or about June 11, 2020, Recruiter 1 issued a check for \$8,000 to Recruiter 2’s business. On or about June 15, 2020, Recruiter 1 deposited the second check from Dessaps, and on or about June 18, 2020, Recruiter 1 issued another check, for \$13,000, to Recruiter 2’s business.

c. Business records indicate that the Internet Protocol (“IP”) address 134.56.24.34 was used to submit the ABC Tech PPP application to Kabbage. Business records from Kabbage and another loan servicer for several SBA-authorized PPP lenders revealed at least 120 additional PPP applications that were submitted from this IP address and/or from the same device (based on common device identification number) between April 2020 and July 2020. These PPP applications were submitted on behalf of business entities and/or self-employed individuals in Florida, Georgia, Maryland, Massachusetts, and New York.

d. Internet service provider records indicate that this IP address was subscribed to an address in Florida neighboring the address of Recruiter 2 during the relevant time period.³ Bank

³ Public records indicate that Recruiter 2 and his spouse resided at an address in Palm Beach Garden, Florida in or around the relevant time period. Public records also indicate that Recruiter

records reflect that Recruiter 2 logged into his personal and business bank accounts from this IP address. Because each of the applications noted above originated from this same IP address, I have concluded that Recruiter 2 submitted each of these PPP applications, including the application for ABC Tech.

e. Investigators searched an email account associated with Recruiter 3 pursuant to a court-issued warrant. Investigators found an email from Recruiter 2's spouse to Recruiter 3, dated June 23, 2020, with the subject line "Commission Report." The body of this email contained a table with columns for "Applicant," "Loan amount," "10% of Loan," "20% Pay," "Agreed Amount," and "Paid out." The applicants listed in the table all were individuals that investigators identified as recipients of loans from applications submitted by Recruiter 2, including Dessaps. The row for Dessaps listed a loan amount of \$800,000 and an "Agreed Amount" of \$20,000. Recruiter 2's spouse also sent Recruiter 3 Excel spreadsheets, labeled "PPP," which listed "Bill: \$836,333" in a tab labeled "Approved" and, in another tab labeled "Declined," the name of Dessaps's brother. Recruiter 3's email account also contained communications between Recruiter 3 and Recruiter 1, to whom Dessaps paid the kickback on ABC Tech's PPP loan from Kabbage.

f. Bank records revealed that borrowers who received PPP funds through applications submitted by Recruiter 2 subsequently made kickback payments to Recruiter 1, Recruiter 2, Recruiter 3, and others. These kickback payments varied but in many cases totaled around 20 percent of the fraudulent loan amount.⁴ In total, I have identified at least \$528,122 in kickback

2 and his spouse were co-owners, managers, and/or officers of three business entities that were registered with the State of Florida at this same Palm Beach Garden address.

⁴ For example, after one business received a PPP loan of \$400,000 in June 2020, the business's owner transferred \$40,000 each to Recruiter 1 and Recruiter 2. After another business received a PPP loan of \$713,793 in July 2020, that business's owner issued two \$71,379 official bank checks from the business account to Recruiter 2 and Recruiter 3. Another business received

payments received by Recruiter 2 and his spouse, \$406,772 in kickback payments received by Recruiter 3, and \$143,760 in kickback payments received by Recruiter 1, all from borrowers who received PPP funds as a result of applications submitted by Recruiter 2.

31. Based on the investigation to date, I have determined that ABC Tech's application to Kabbage vastly overstated ABC Tech's 2019 employees and payroll expenses:

a. In addition to the prior PPP applications that Dessaps submitted to TD Bank and Eastern Bank, ABC Tech also submitted two applications to the SBA for Economic Injury Disaster Loan ("EIDL") funds in 2020. On or about April 2, 2020, ABC Tech submitted an application that indicated that ABC had two employees as of January 31, 2020 and gross revenues of \$1,919,503 and total cost of goods sold of \$1,463,458 for the twelve months prior to January 31, 2020. On or about December 21, 2020, ABC Tech submitted another EIDL application, which indicated that ABC had two employees as of January 31, 2020. For the twelve months prior to January 31, 2020, the December EIDL application stated gross revenues of \$3,716,364 and a cost of goods sold of \$2,492,711. In contrast with these amounts, the PPP application to Kabbage reported over \$3.8 million in 2019 payroll expenses alone.

b. Records from the Massachusetts Department of Revenue indicate that ABC Tech reported, for the second quarter of 2020 (during which Kabbage received the PPP application), 12 employees and gross wages of \$27,616 (approximately \$9,205 per month).

c. Tax return information indicates that Dessaps did not file employment tax returns for ABC Tech for the tax year 2019.

a PPP loan of \$800,000 through a PPP application submitted through Recruiter 2, and the business owner subsequently caused three checks, each for \$80,000, to be issued to Recruiter 2, Recruiter 3, and a third individual who initially approached the business owner about submitting an application.

d. Bank records for ABC Tech do not reflect the payroll activity represented on the PPP application. While Dessaps did, in fact, operate ABC Tech as a used car dealership and employ individuals at the dealership, ABC Tech's bank statements and other documents I have reviewed indicate that, in 2019, ABC Tech did not issue regular paychecks to employees and appeared to employ only a small handful of individuals. The income and expenses reflected in the bank records appear consistent with a modest used car dealership, not a dealership with 40 employees and yearly payroll expenses of \$3.8 million.

32. Based on my training and experience, I know that the Form W-3 that was submitted for ABC Tech was fabricated:

a. Employers submit quarterly Forms 941 to the IRS that report information about wages paid to employees. That information corresponds to employment data that employers summarize on Forms W-3. I have reviewed IRS records with respect to Dessaps pursuant to an *ex parte* order, and those records do not include any Forms 941 or W-3.

b. The amounts reported on the Form W-3 submitted to Kabbage are inconsistent with other IRS forms that Dessaps submitted in support of other applications, as described above.

c. Additionally, the Form W-3 exhibits several infirmities. Social Security and Medicare taxes should be a fixed percentage of the associated wages (6.2% and 1.45% respectively) and should not be the same amount as the associated wages, as they are listed on the Form W-3 for ABC Tech that was submitted to Kabbage. Additionally, because there is no cap on the amount of Medicare wages that are taxable, Medicare wages should be equal to or greater than the gross wages of \$3,840,000. Moreover, the Form W-3 also reported state taxes withheld of \$176,640 but no state wages. I have reviewed supporting documents for other PPP loan

applications submitted through Recruiter 2, and I have observed numerous Forms W-3 with similar discrepancies that were submitted with these loan applications.

Misuse of PPP Funds

33. Bank records indicate that, after receiving the \$836,800 in PPP funds from Kabbage, Dessaps made the two kickback payments of \$14,000 to Recruiter 1, noted above.

34. Dessaps also made a series of payments disguised as payroll checks. Bank records reflect that, on or about June 11, 2020, Dessaps opened a new bank account with TD Bank for ABC Tech (the “Payroll Account”) and transferred \$750,000 from the ABC Tech operating account that had received the Kabbage PPP funds into the new Payroll Account. Between June 23, 2022 and August 13, 2020, Dessaps used the funds in the Payroll Account to issue checks that resembled paychecks from ABC Tech to 11 individuals, totaling \$59,589.37. Prior to receiving PPP funds, ABC Tech had not issued any checks of this kind, and ABC Tech issued no further checks of this kind after August 12, 2020. These checks included checks written to Dessaps personally (totaling \$15,570), his brother (totaling \$17,295), his sister (totaling \$7,223.60), and eight individuals outside his family (totaling \$19,500.41). Six of the eight non-family payees also received one-time checks ranging in amount from \$3,600 to \$4,000, and one of these individuals endorsed her payments to Dessaps’s brother or his brother’s wife. ABC Tech made two additional payments to Dessaps’s brother totaling \$10,000. Dessaps’s brother subsequently issued a check for approximately \$26,000 to Dessaps on or about September 11, 2020. Based on my training and experience, I believe that Dessaps issued these paychecks to create the appearance of payroll, for the purpose of a future PPP loan forgiveness application, and that Dessaps’s brother and other individuals returned most of this money to Dessaps.

35. Based on my review of bank records, other financial records, and public documents, I have determined that Dessaps spent a substantial portion of the PPP loan from Kabbage on a new residence for himself:

a. On or about August 4, 2020, Dessaps's sister signed a purchase and sale agreement to purchase the Subject Premises for \$750,000 and paid a deposit of \$30,000 from the joint account she shared with Dessaps.

b. Based on my experience, I am aware that issuers of mortgages usually require documentation of the source of funds to be used to complete the purchase of real estate, up to and including the source of recent deposits to the purchaser's bank accounts. The financial institution typically checks whether the funds were on deposit and available prior to the loan.

c. In support of the mortgage application, Dessaps's sister submitted a purported copy of a 2019 Form W-2 from ABC Tech that indicated that the business had paid wages of \$104,000 to Dessaps's sister during 2019. However, IRS records indicate that ABC Tech filed no reports of wages and/or Forms W-2 to the IRS, and no bank records for ABC Tech support the claim that ABC Tech paid Dessaps's sister \$104,000 in 2019. Dessaps's sister also submitted a purported copy of 2019 IRS Form 1040-X (Amended U.S. Individual Income Tax Return), dated August 15, 2020, which reported additional income from ABC Tech, in addition to her income from her actual employment, resulting in total gross income of \$174,262 for 2019. However, IRS records indicate that no amended tax form for Dessaps's sister was actually filed for 2019.

d. The mortgage application also included a copy of a bank statement for a family friend's checking account, which purported to show a beginning balance on August 21, 2020 of \$134,225.60 and an ending balance on September 21, 2020 of \$136,357.59. However, actual bank records for the family friend's account show that the beginning balance on August 21, 2020 was

\$4,119.07 and the ending balance on September 21, 2020 was only \$6,144.11. Based on this discrepancy and the payment from ABC Tech to the family friend, I believe that Dessaps arranged for the submission a falsified bank statement for the family friend to the mortgage lender.

e. The supporting documentation also included records purporting to show that Dessaps's sister received proceeds from the sale of two vehicles to ABC Tech—a BMW, purportedly sold to ABC Tech for \$51,900 on or about September 10, 2020, and a Porsche, purportedly sold to ABC Tech for \$33,000. For the Porsche, Dessaps issued a bank check for \$33,000 from the Payroll Account, which was deposited into his and his sister's joint account. For the BMW, Dessaps issued a bank check for \$51,900 from another ABC Tech bank account into which he had transferred PPP proceeds. Investigators confirmed that the VINs provided for these vehicles were accurate VINs for real automobiles registered with the Commonwealth of Massachusetts. However, investigators found no record that Dessaps's sister ever owned the BMW. Further, records for the joint bank account for Dessaps and his sister reflect that the account received a check deposit for \$25,000 on or about October 18, 2018, payable to Dessaps's sister. The check was from an automobile dealership and stated in the memo line: "Purchase 2010 Porsche Panam, VIN: 090351" (reflecting the same VIN as the VIN for the vehicle that the supporting documentation purported to show that Dessaps later purchased from his sister). Based on my training and experience and the investigation to date, I believe that Dessaps fabricated these car purchases as a pretense for transferring money to his sister to support the mortgage application.

f. On or about September 16, 2020, Dessaps purchased an official bank check in the amount of \$36,000 issued to his sister. The source of funds for the bank check was another ABC Tech bank account that had received the PPP funds that had been paid to Dessaps personally from ABC Tech and the funds that returned to Dessaps from his brother. The bank check was deposited

to the joint account and presented to the mortgage company as a purported “gift” to Dessaps’s sister for the purchase of the Subject Premises.

g. Between October 20 and 21, 2020, Dessaps wired 4 payments totaling \$127,500 into an account of the family friend from ABC Tech’s bank accounts and the joint account he shared with his sister. On or about October 22, 2020, the family friend wired \$127,500 to the closing attorney for the purchase of the Subject Premises. This transaction was presented to the mortgage company as “gift” from the family friend to Dessaps’s sister for the down payment of the Subject Premises. The remainder of the approximately \$250,000 in down payment and closing costs was paid from the joint account that Dessaps’s sister and Dessaps shared.

36. Investigators have conducted surveillance of the Subject Premises and observed that Dessaps is the full-time resident of the Subject Premises. Investigators also confirmed that Dessaps’s sister has continued to reside at her prior address in North Attleboro.

37. From the foregoing information, there is probable cause to believe that Dessaps transferred fraudulently obtained PPP funds to his sister and to the family friend for the purpose of purchasing the Subject Premises and obtaining a mortgage, both in his sister’s name, thereby concealing his use of PPP funds on a new residence.

38. Bank records indicate that Dessaps also spent PPP funds on other personal expenses, including, but not limited to, French bulldogs. Between October 2, 2020 and January 14, 2021, ABC Tech’s bank accounts issued three payments totaling \$32,000 to West Virginia-based breeders of French Bulldogs.

39. Bank records also indicate that Dessaps also spent PPP funds on the Rolls Royce. Between October 15 and November 19, 2020, Dessaps made four payments totaling \$133,000 to

a business that appeared to buy and resell automobiles. Based on the payment history and related communications, I believe that these funds were used to purchase the Rolls Royce.

40. For example, an attempted payment, which was not completed, was a \$10,000 check with a memo line that read: “For 2014 Benley [sic] Wraith VIN SCA665c54EUX84578.”⁵ The first completed payment was a \$10,000 wire transfer on October 19, 2020, from the bank account that received the PPP funds from Kabbage, with a wire memo that read: “Roll [sic] Royce.” Dessaps made the second payment—another \$10,000 wire transfer from the bank account that received the PPP funds from Kabbage—on or about November 12, 2020. The third payment, a \$90,000 wire on or about November 19, 2020, came from another bank account that received a \$90,000 loan from a financing company that same day. The final deposit, a \$23,000 cashier’s check, appears to have been paid for in cash. Based on my review of bank records and knowledge of the investigation, I believe that this cashier’s check was purchased at least in part from cash withdrawn from the account that received the PPP funds from Kabbage.

41. A VIN search confirmed that the business to which Dessaps was sending the payments previously had purchased the Rolls Royce for \$110,000 on October 13, 2020. Investigators spoke with local law enforcement officers, who have observed Dessaps driving the Rolls Royce and parking the Rolls Royce in ABC Tech’s lot on multiple occasions, including in February 2021. On or about October 20, 2022, I observed the Rolls Royce on the driveway at the Subject Premises. On or about November 19, 2022, the Randolph Police Department received a report regarding Dessaps, whom the complainant stated had driven a black Rolls Royce to the

⁵ The reference to “Benley” in the memo line of this first payment likely reflects a mistaken belief that Bentley, rather than Rolls Royce, manufactured the Wraith model.

complainant's workplace that day. Officers observed the Rolls Royce at the Subject Premises the following day.

42. Vehicle registration records indicate that, on or about October 20, 2022, Dessaps assigned the certificate of title to the Rolls Royce to Dessaps's brother's company. Dessaps's brother purported to sell the Rolls Royce to Dessaps's sister on or about November 20, 2022 and re-assigned the certificate of title to Dessaps's sister on or about November 28, 2022.

43. Based on my review of documents and my knowledge of the investigation, I believe the purported sale to Dessaps's sister was a sham transfer. According to the corresponding Registration and Title Application filed with the Massachusetts Registry of Motor Vehicles, Dessaps's sister allegedly financed the purchase of the Rolls Royce in part through a trade-in of a 2013 Porsche Cayenne; however, other vehicle records indicate that the Porsche Cayenne had been registered to another individual at least five months prior to Dessaps's sister's purported purchase of the Rolls Royce. As described above, Dessaps previously purchased the Subject Premises in his sister's name but then enjoyed sole residence at the Subject Premises. Moreover, investigators have observed Dessaps driving the Rolls Royce and the Rolls Royce parked on the driveway at the Subject Premises as recently as November 20, 2022.

44. Based on the above, I have probable cause to believe Dessaps used more than \$10,000 in fraudulent PPP loan proceeds, transferred from the TD Bank account that had received those proceeds, to purchase the Rolls Royce, in violation of 18 U.S.C. § 1957(a). Accordingly, I believe that there is probable cause that the Rolls Royce represents property derived from a wire fraud violation and/or property involved in a money laundering transaction or property traceable to such property.

Probable Cause to Search the Subject Premises

45. There is also probable cause to believe that the Subject Premises will contain fruits, evidence, and instrumentalities of violations of the Target Offenses, as described in Attachment B to the proposed warrant to search the Subject Premises. Specifically, there is probable cause to believe that the Rolls Royce and the Subject Device will be located at the Premises.

46. Based on surveillance of Dessaps and the Subject Premises conducted as recently as October 20, 2022, I have determined that Dessaps resides at the Subject Premises, notwithstanding his sister's formal ownership of the Subject Premises. Additionally, recent utilities bills have been addressed to Dessaps at the Subject Premises, and Dessaps's most recent annual corporate filing for ABC Tech, made on July 20, 2022, listed the Subject Premises as his address. I am not aware of any other location where Dessaps might reside.

47. Based on the investigation to date, I believe that Dessaps used the Subject Device to communicate with Recruiter 1 about the fraudulent PPP application submitted to Kabbage. Telephone records indicate that Dessaps first spoke by phone with Recruiter 1 on June 3, 2020, the day that the application was submitted. Records indicate that, before Recruiter 1 contacted Dessaps, Recruiter 1 spoke with another Massachusetts-based individual with whom both Recruiter 1 and Dessaps communicated by phone frequently. After an initial call from Recruiter 1 to Dessaps, the two exchanged several more calls and text messages on June 3, 2020, as well as calls and text messages on several other occasions throughout the remainder of June 2020.

48. Based on my training and experience, I am aware that mobile phone users typically correspond with other individuals through both phone calls and text messages. I also am aware that mobile phone users typically keep their mobile phones on their persons or, while at home, elsewhere in their residences.

49. Bank records reflect that Dessaps listed the number for the Subject Device on the PPP applications submitted to TD Bank and in statement records maintained by Eastern Bank, and that the number for the Subject Device was provided in the fraudulent PPP application submitted to Kabbage.

50. Based on surveillance, financial records, and information from the Abington police department, I also have determined that Dessaps possesses and drives the Rolls Royce.

51. I have observed the Rolls Royce parked on the driveway of the Premises. I am not aware of any other location where Dessaps might store the Rolls Royce.

Seizure of Computer Equipment and Data

52. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

53. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

54. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes

automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session

times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein

may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

55. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence – storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements – analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and

its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

56. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

57. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) Dessaps. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law

enforcement agents will seize that device pursuant to the probable cause established herein and seek additional authority to search it.

Unlocking a Device Using Biometric Features

58. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

59. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

60. The passcode that would unlock the Subject Device is not currently known to law enforcement. Thus, it may be useful to press Dessaps's fingers to the device's fingerprint sensor or to hold the device up to Dessaps's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to

access the data contained on those devices for the purpose of executing the search authorized by this warrant.

61. For these reasons, I request that the Court authorize law enforcement to press Dessaps's fingers (including thumbs) to the sensor of the Subject Device or place the Subject Device in front of Dessaps's face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

SEIZURE AUTHORITY

62. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, specifically, 18 U.S.C. § 1343 (wire fraud), is subject to forfeiture. Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity.

63. Pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1), any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957, or 1960 of this title, or any property traceable to such property, is subject to forfeiture.

64. This Court has authority to issue a civil seizure warrant pursuant to 18 U.S.C. § 981(b)(2), which states that “[s]eizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure.” This Court also has authority to issue the requested criminal seizure warrant pursuant to 21 U.S.C. § 853(f), as incorporated by 28 U.S.C. § 2461(c), which authorizes “the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant.”

65. This Court has jurisdiction to enter the requested seizure warrant in the District of Massachusetts because a forfeiture action may be filed in this District. *See* 28 U.S.C. § 1335 (“A forfeiture action or proceeding may be brought in—(A) the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred, or (B) any other district where venue for the forfeiture action or proceeding is specifically provided for.”); Fed. R. Crim. P. 41(b) (magistrate judge has authority to issue a warrant to seize property “located in the district” and, “in any district where activities related to the crime may have occurred[, to] issue a warrant for property that is located outside the jurisdiction of any state or district.”).

66. Based on my training and experience, seizure warrants are required in order to restrain vehicles because vehicles can be concealed, destroyed, or removed from the jurisdiction with relative ease.

CONCLUSION

67. Based on the information described above, I have probable cause to believe that that Dessaps has violated 18 U.S.C. §§ 1349 and 1956(h) in connection with his submission of fraudulent loan applications and engagement in financial transactions with the fraudulently obtained loan proceeds.

68. I also have probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachment B to the proposed warrant to search the Subject Premises, are contained within the premises described in Attachment A.

69. Further, there is probable cause to believe that the Rolls Royce was purchased in part with proceeds traceable to wire fraud and is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 982(a)(1), and 28 U.S.C. § 2461(c).

Sworn to under the pains and penalties of perjury,


Than Nguyen
Special Agent
IRS, Criminal Investigation

Sworn to via telephone in accordance with Federal Rule of
Criminal Procedure 4.1 on January ~~2023~~
Jan 24, 2023


Hon. Judith G. Dein
United States Magistrate Judge

23-5014-JGD
23-5016-JGD
23-5019-JGD